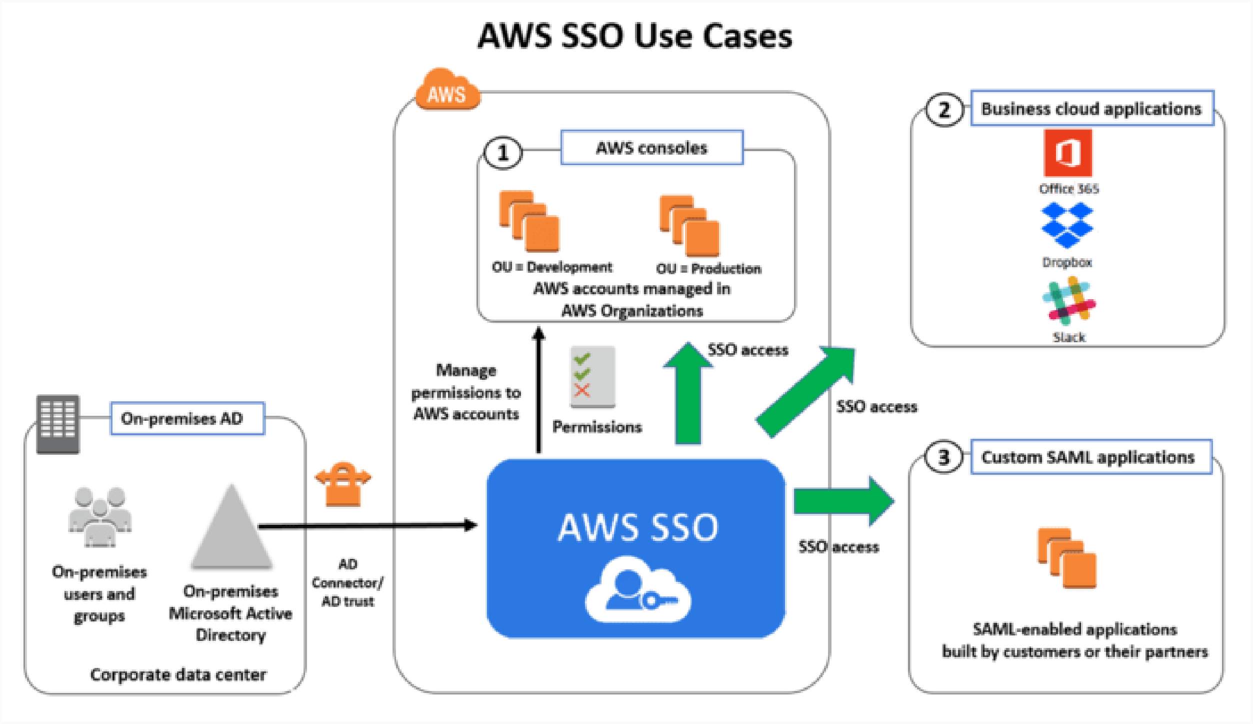
What is SSO?

Single sign-on (SSO) is an authentication solution that allows users to log in to multiple applications and websites with one-time user authentication. Given that users today frequently access applications directly from their browsers, organizations are prioritizing access management strategies that improve both security and the user experience. SSO delivers both aspects, as users can access all password-protected resources without repeated logins once their identity is validated.

Why is SSO important?

Using SSO to streamline user logins benefits users and organizations in several ways.


AWS SSO Use Cases
AWS
1
AWS consoles
OU = Development
OU = Production
AWS accounts managed in AWS Organizations
2
Business cloud applications
Office 365
Dropbox
Slack
Manage permissions to AWS accounts
Permissions
SSO access
SSO access
SSO access
On-premises AD
On-premises users and groups
On-premises Microsoft Active Directory
Corporate data center
AD Connector/ AD trust
AWS SSO
3
Custom SAML applications
SAML-enabled applications built by customers or their partners

Strengthen password security

When people don’t use SSO, they must remember multiple passwords for different websites. This might lead to non-recommended security practices, such as using simple or repetitive passwords for different accounts. Besides, users might forget or mistype their credentials when logging in to a service. SSO prevents password fatigue and encourages users to create a strong password that can be used for multiple websites.

Improve productivity

Employees often use more than one enterprise application that requires separate authentication. Manually entering the username and password for every application is time-consuming and unproductive. SSO streamlines the user validation process for enterprise applications and makes it easier to access protected resources.

Reduce costs

In their attempt to remember numerous passwords, enterprise users may forget their login credentials. This results in frequent requests to retrieve or reset their passwords, which increases workload for the in-house IT teams. Implementing SSO reduces occurrences of forgotten passwords and thus minimizes the support resources in handling requests for password resets.

Improve security posture

By minimizing the number of passwords per user, SSO facilitates user access auditing and provides robust access control to all types of data. This reduces the risk of security events that target passwords, while helping organizations comply with data security regulations.

Provide a better customer experience

Cloud application vendors use SSO to provide end-users with a seamless login experience and credential management. Users manage fewer passwords and can still securely access the information and apps they need to complete their day-to-day jobs.

How does SSO work?

SSO establishes trust amongst the application or service and an external service provider, also known as an identity provider (IdP). This happens through a series of authentication, validation, and communication steps carried out between the application and a centralized SSO service. The important components in SSO solutions are given below.

SSO service

An SSO service is a central service that applications rely on when a user logs in. If an unauthenticated user requests access to an application, the app redirects them to the SSO service. The service then authenticates and redirects the user back to the original application. The service typically runs on a dedicated SSO policy server.

SSO token

An SSO token is a digital file that contains user-identifying information, such as a username or email address. When a user requests access to an application, the application exchanges an SSO token with the SSO service to authenticate the user.

SSO process

The SSO process is as follows:

1. When a user signs in to an application, the app generates an SSO token and sends an authentication request to the SSO service.
2. The service checks if the user was previously authenticated in the system. If yes, it sends an authentication confirmed response to the application to grant access to the user.
3. If the user does not have a validated credential, the SSO service redirects the user to a central login system and prompts the user to submit their username and password.
4. Upon submission, the service validates the user credentials and sends the positive response to the application.

5. Otherwise, the user receives an error message and must re-enter credentials. Multiple failed login attempts could result in the service blocking the user from further attempts for a fixed period of time.

What are the types of SSO?

There are different standards and protocols that SSO solutions use to validate and authenticate user credentials.

SAML

SAML, or Security Assertion Markup Language, is a protocol or set of rules that applications use to exchange authentication information with the SSO service. SAML uses XML, a browser-friendly markup language, to exchange user identification data. SAML-based SSO services provide better security and flexibility, as applications do not need to store user credentials on their system.

OAuth

OAuth, or Open Authorization, is an open standard that allows applications to securely gain access to user information from other websites without giving them the password. Instead of requesting user passwords, applications use OAuth to gain user permission to access password-protected data. OAuth establishes trust between applications through API, which allows the application to send and respond to authentication requests in an established framework.

OIDC

OpenID is a way to use a single set of user credentials to access multiple sites. It allows the service provider to assume the role of authenticating the user credentials. Instead of passing an authentication token to a third-party identity provider, web applications use OIDC to request additional information and validate the user’s authenticity.

Kerberos

Kerberos is a ticket-based authentication system that lets two or more parties mutually verify their identity on the network. It uses security cryptography to prevent unauthorized access to identification information transmitted amongst the server, clients, and Key Distribution Center.

Is SSO secure?

Yes, SSO is an advanced and desirable identity access management solution. When deployed, a single sign-on solution helps organizations with user access management for enterprise applications and resources. An SSO solution makes setting and remembering strong passwords easier for application users. In addition, the IT team can use the SSO tool to monitor user behavior, improve system resilience, and reduce security risks.

How does SSO compare with other access management solutions?

There are several identity and access management solutions you can choose from, depending on your requirements.

Federated identity management

Federated identity management (FIM) is a digital framework that allows multiple applications from different vendors to share, manage, and authenticate user identity. For example, FIM allows your workforce to login to one application and then access several other enterprise applications without logging in again. FIM authenticates the credential submitted from the service provider with a credible identity provider.

SSO vs. federated identity management

Federated identity management is a comprehensive identity authentication and management solution for cross-domain applications. Meanwhile, single sign-on (SSO) is a specific functionality within the FIM model. While FIM allows users to access services from different vendors with a single login, SSO is limited to services or applications hosted by a single vendor.

Same sign-on

Same sign-on, which also bears the SSO acronym, is a digital solution that stores and synchronizes user credentials on devices accessed by the user. It is similar to password vaults or password managers that allow users to sign in to multiple apps on different devices without remembering the credentials.

Single sign-on vs. same sign-on

Single sign-on systems require a one-time authentication from the user. Once logged in, the user can access other web applications and services without re-authenticating themselves. Meanwhile, same sign-on requires the user to repeat the login process each time with the same authentication credentials.

Multi-factor authentication

Multi-factor authentication is a user authentication framework using two or more technologies to verify the user’s identity. For example, users enter their email address and password on a webpage and key in a one-time password (OTP) sent to their mobile phone to enable secure access.

SSO vs. multi-factor authentication

SSO enables organizations to simplify and strengthen password security by allowing access to all connected services with a single login. Multi-factor authentication provides additional security layers to reduce the possibility of unauthorized access through stolen credentials. Both SSO and multi-factor authentication can be integrated to improve the security posture of web applications.

How can AWS help with SSO?

AWS IAM Identity Center is a cloud authentication solution that allows organizations to securely create or connect their workforce identities and manage their access centrally across AWS accounts and applications. You can create user identities or import them from external identity providers such as Okta Universal Directory or Azure. Some benefits of AWS IAM Identity Center include:

- A central dashboard to manage identities for your AWS account or business applications.
- Multi-factor authentication support to provide a highly secure authentication experience for users.
- Integration support with other AWS applications for zero-configuration authentication and authorization.

Get started with SSO on AWS by creating a free AWS account today.